Lecture 8: CRT, XGCD, and Inverses Modulo N

§1 CRT

Theorem (CRT):

$a, b \in \mathbb{Z}$ $\quad n, m$ "coprime" (i.e. $\gcd(n,m)=1$)

There's a unique solution x (mod nm) to

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}.$$

Proof: Exist: Solve $a + mt \equiv b \pmod{n}$ for t and let $x = a + mt$.

Unique: x, x' both soln's.

$$\left.\begin{array}{l} x - x' \equiv 0 \pmod{m} \\ x - x' \equiv 0 \pmod{n} \end{array}\right\} \Rightarrow n, m \mid x - x'$$

$$\Rightarrow x \equiv x' \pmod{mn}.$$

But how do we solve $a + mt \equiv b \pmod{n}$ for t?

$$mt \equiv b - a \pmod{n}.$$

1. Find m' such that $m'm \equiv 1 \pmod{n}$
2. Multiply both sides by m':

$$m'mt \equiv t \equiv m'(b-a) \pmod{n}.$$

So: Problem is reduced to a new problem

Problem: Given a and n with $\gcd(a,n) = 1$,
Find x with $ax \equiv 1 \pmod{n}$.

This would solve everything.

We know x exists:

$$\mathbb{Z}/n\mathbb{Z} \hookrightarrow \mathbb{Z}/n\mathbb{Z}$$
$$x \longmapsto ax$$

injective map of finite sets is a bijection.

since $ax \equiv ax' \pmod n \Rightarrow x \equiv x' \pmod n$

(which we prove by $a(x-x') \equiv 0 \pmod n \Rightarrow n \mid a(x-x') \Rightarrow n \mid (x-x')$)

But how to compute?

§2 XGCD.

Prop: $a, b \in \mathbb{Z}$, $g = \gcd(a,b)$

There exists x, y s.t.

$$ax + by = g.$$

Proof. $\gcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1$ so $\frac{a}{g}x \equiv 1 \left(\bmod \frac{b}{g}\right)$ has a solution.

So $\frac{b}{g}(-y) = \frac{a}{g}x - 1$ for some y.

So $-by = ax - g \Rightarrow g = ax + by$, as claimed. $\square$

Fact: There is a fast algorithm to compute such x and y.

Example:

$a=5, \quad b=7$

$7 = 1\cdot 5 + 2 \qquad\qquad a = qb + r$

$5 = 2\cdot 2 + 1 \quad \Rightarrow \quad 1 = 5 - 2\cdot 2$

$\qquad\qquad\qquad\qquad\qquad = 5 - 2\cdot(7 - 1\cdot 5)$

$\qquad\qquad\qquad\qquad\qquad = 3\cdot 5 - 2\cdot 7$

so $x = 3$, $y = -2$.

Idea of algorithm:

run gcd algorithm, then back substitute to get x, y.

Example: $a = 130, \quad b = 59$

$130 = 2\cdot 59 + 12 \quad \Rightarrow \quad 12 = 130 - 2\cdot 59$

$59 = 4\cdot 12 + 11 \quad \Rightarrow \quad 11 = 59 - 4\cdot 12$

$\qquad\qquad\qquad\qquad\qquad = 59 - 4\cdot 130 + 8\cdot 59 = 9\cdot 59 - 4\cdot 130$

$12 = 1\cdot 11 + 1 \quad \Rightarrow \quad 1 = 12 - 1\cdot 11$

$\qquad\qquad\qquad\qquad\qquad = 130 - 2\cdot 59 - (9\cdot 59 - 4\cdot 130)$

$\qquad\qquad\qquad\qquad\qquad = 5\cdot 130 - 11\cdot 59$

$5\cdot 130 - 11\cdot 59 = 1 \quad (= \gcd(a,b))$.

How to compute inverse of a (mod n).

① Since $\gcd(a,n)=1$ we can compute x, y such that

$$ax+ny=1.$$

② Then $a\underline{x} \equiv 1 \pmod{n}$.

Ex: $a=59$, $n=130$.

$$(-11)59 + 5\cdot 130 = 1$$

so $x=-11$ is inverse of $a=59$ mod 130.

Application to CRT:

Find x such that

$$x \equiv 3 \pmod{19}$$
$$x \equiv 5 \pmod{13}.$$

Solution: We solve $a+mt \equiv b \pmod{n}$, so $x \equiv a+mt$.

$$3+19t \equiv 5 \pmod{13}$$
$$19t \equiv 2 \pmod{13}$$
$$6t \equiv 2 \pmod{13}$$

Find x, y with.

$$6x+13y=1$$

$\underline{13} = 2\cdot\underline{6}+\underline{1}$

so $x=-2$, $y=1$ works.

so $(6 \bmod 13)^{-1} \equiv -2$

$$-2\cdot 6t \equiv -2\cdot 2 \pmod{13}$$
$$t \equiv 9 \pmod{13}$$

So $x = 3+19\cdot 9$
$= 174$